Hearing Before The

U.S. Senate Committee on the Judiciary
Subcommittee on Technology, Terrorism, and Government Information
226 Dirksen Senate Office Building
Washington, D.C.

22 May 2001

Verification of Network Activity and Effective Security Policy: Technology and Management Solutions

Testimony Of

Dr. Taher Elgamal
Chairman, President & CEO
Securify, Inc.

Contact Information:
Peter F. Harter
Senior Vice President
Business Development & Public Policy
Securify, Inc.
1157 San Antonio Road
Mountain View, CA 94303-1002 USA
peter@securify.com
http://www.securify.com/
+1.917.640.2016 Mobile
+1.650.812.9400 ext. 4186 Office
+1.650.812.9410 Fax

Verification of Network Activity and Effective Security Policy:

Technology and Management Solutions

Executive Summary

Protecting our nation's critical infrastructures today is a great challenge given the open and global nature of the Internet. Since the Internet was not developed for commercial activity and since it does not recognize political borders, industry and government need to invest in new technologies and business practices in order to strengthen the Internet. Obviously more and more value resides online in networks. Increasingly, society itself is dependent upon computer-based communications and the Internet.

Greater coordination between governments and industry is necessary. Information sharing and analysis is a good start. However, security needs to become a tool for running one's business or organization in a more effective manner, rather than a reaction to a problem. Fundamentally, security is first about being aware of what is actually happening on one's network. Simply putting up barriers at the perimeter of your network is not going to work. There are no walls in cyberspace: remote access by employees, consultants on site, and ever increasing interconnectedness with other networks eliminate any sense of walls. Rather than defending one's network from perceived outside threats, one must instead manage from the inside outward. Vigilance rather than repair will become the standard operating procedure for both industry and government networks.

.

Verification of Network Activity and Effective Security Policy:

Technology and Management Solutions

Introduction

Protection of our nation's critical infrastructure requires increased attention from business and government. With the advent of the Internet more of society is dependent on computer-based communications. This will not change. Globalization, economic productivity, trade, innovation, education, and other drivers accelerate dependency. Since the private sector owns or operates the vast majority of the world's information infrastructure and relies upon other infrastructures (e.g., energy, law enforcement, health care, finance, transportation, defense) that are recognized in many cases as government driven, both industry and government must cooperate closely on the significant issues before the Subcommittee today.

Securify, Inc., is pleased to be a witness. We believe that our approach to security enables business and government to be in a superior position to address today's infrastructure concerns. From my own professional experience I know first hand about the close working relationships between industry and government in the area of security. For example, my PhD thesis became the adopted DSS government standard for digital signatures. Based on this experience I respectfully suggest some public policy ideas for the Subcommittee to consider.

Background on Securify, Inc.

One cannot have security without the ability to continually verify that actual activity comports with expectations, rules and policies. One can spend a lot of time and money on people and technology and not improve the quality of security. Verification is an essential and logical first step.

Securify was founded in 1998 as VeriGuard, Inc. Within the first 10 months the company changed its name to Securify and was then sold to Kroll-O'Gara, a publicly traded risk mitigation and security services firm. Kroll-O'Gara spun Securify out as an independent company in 2000. Today Securify is a privately held firm with approximately 100 employees. Our headquarters are based in Mountain View, California.

Securify began as a high-end information security consulting firm. Clients were Fortune 50 firms with very sensitive security needs. Early on Securify recognized that customers needed automated, technology driven and continuous security solutions. Customer needs escalated and outstripped the availability of security experts and consumed increasing portions of IT budgets. A proactive, cost-effective approach that served the business needs of the customer was necessary. For nearly two years Securify has researched and developed a unique, patent-pending technology. It is called SecurVantage.

Securify designed this unique, managed service for measuring security effectiveness of business networks including intranets, production networks and connections to the networks of partners, customers and suppliers. Securify SecurVantage provides in-depth visibility and analysis of the security attributes of live network traffic, enabling security managers and IT staff to quickly detect misconfiguration, and the presence of unauthorized devices.

Most organizations manage each security device independently and hope the combination of devices provides security. Securify SecurVantage provides a continuous method for comparing real time traffic to business-level security standards. Performing this analysis of real time traffic on a continuous basis is the best method to ensure live traffic is conforming to corporate security guidelines. Securify SecurVantage provides a high-level overview of security policy development, implementation, and continuous maintenance. It quickly targets inconsistencies and recommends corrective actions. Securify SecurVantage establishes a baseline, customized, business-driven security policy specification for each customer. Using this specification, network traffic is analyzed for conformance to the desired security requirements. If a violation is detected, the Securify Network Operations Center (NOC) staff alerts the customer of the violation and recommends corrective action. Securify SecurVantage can also be used to establish metrics to ensure traffic flowing between business partners meets required security parameters. This is particularly important for companies that rely on their distributed networks for day-to-day operations, wherever valuable data is accessed and stored.

What Is Needed To Protect Critical Infrastructures: Verification and Security

Securify's SecurVantage demonstrates the combination of security and verification. By continually verifying that the activity on your networks and the networks you connect to is what is expected, then one can focus on mitigating the deviations, anomalies, deviations and exceptions. This is a significantly smaller set of events to focus on than the ever evolving and growing universe of threats and vulnerabilities. Rather than reacting to the expanse of threats and vulnerabilities one can mitigate risk on a level that is customized and do so in an intelligent and managed manner. It is the difference between reacting on little or no information to acting according to a plan. And since this approach is a part of the every day functioning of the customer's business and their networks, they have the ability to assess security performance and other network attributes. So it is more than security; it helps make the network and the organization it serves healthier, more reliable and productive. It simply makes it more valuable.

This is an important point. Government and business increasingly have more value and more at stake digitally than physically. Assets and value are based not on material objects but on information assets and network connections. From General Electric to Dell, from old to new, more businesses are using technology to change how they're run and to manage their operations and relations with employees, customers, suppliers and partners. More revenue is derived from network activity. More cost savings are gained from online activity. Today this is no longer headline news but a real fact of life for business and government alike.

We all recognize that an organization cannot function properly, effectively, successfully, competitively or legally without sound financial management processes and systems. A business cannot function if it does not continually know the status of money coming in and money going out and who it touching the money. The same has become true for network activity and the increasingly valuable and critical information that flows through the network. Even today, discussions of corporate network security issues are delegated down from corporate management to the IT department. Recent reports by the GAO on the status of government network operations reveal a similar problem. We believe that a healthy dialogue between senior government officials, corporate CEOs and Boards of Directors, academia and others is required if these issues are to be appropriately addressed and resolved.

As a vendor of security technology and solutions, Securify of course stands to benefit from spending on security by business and government. Securify is not here today to recite the latest statistics on the number of attacks and threats and their cost to business and our economy. Frankly, the damage done by overt activity is overshadowed by the costs resulting from poorly managed networks.

Securify advocates the adoption of the proactive and continuous approach of verification. It is simply good business and trustworthy government. One cannot manage what they do not measure. If one does not have a network security policy in place and if one does not continually measure the actual activity on the network against this policy, then one

will never know if they are secure. As a result the network is unreliable and it cannot ensure privacy, security, and integrity.

It is important to note that the Internet was designed some thirty years ago by collaboration between government, industry and academia. The Internet was designed to be an open medium for sharing information. Security and commercial activity were not a part of the original programming. It is important to recognize this plain fact. Now that we are all dependent on the Internet and computer-based communications we need to take some new action to make the Internet strong enough.

Action includes increased information sharing and analysis within industry and government. Action includes adopting new technologies and business practices. Spending on security has not really diminished in the current economic climate. A recent survey of the chief information officers of the Fortune 100 reported that security spending is the last item to be cut from an IT budget. This may be stating the obvious. One does not cut what protects one's assets. What is not so obvious is that security spending has increased in recent years but no one really knows how effective those investments have been.

If one can start from the first point of a verified network then the owner and operator of that network has the ability to continually ensure that it is functioning within expected parameters. They can track activity and correct errors and analyze historical records for improvement and modification. Results of this include greater reliability (i.e., less network downtime), privacy assurance (i.e., one has the ability to determine if the set

privacy rules and practices are being applied properly and followed) and greater security (i.e., one can track deviations and anomalies in real time across all networks).

This is not some sort of big brother technology. It is a business tool. Just as a senior management team and a board of directors must know if there is a misuse of funds or property or some sort of illegal activity taking place inside their company, they must have the tools and ability to detect and mitigate the same sorts of unauthorized activity in the digital world. Such a tool provides for transparency in the operation of a business. Without it truly nefarious activity would be able to flourish and do so unchecked as no one would be readily able to detect it or mitigate it.

By using SecurVantage our customers immediately see unauthorized activity such as an employee using a file server to transmit sensitive data to a competitor. Employees and consultants use a network and its resources to run gambling and pornography businesses. Many misuse their access to peruse parts of the network they don't need to see or should not gain access to. These are just a few examples. But they easily illustrate the costs of misuse of a network. From just the cost control perspective, network misuse increases operating costs. Why should a company pay for more bandwidth, energy, equipment or technical support than it has to in order to do its business? Again, security is really about running an organization correctly and effectively. It is not simply a matter of preventing attacks or locking secrets away. At some point, financial audits are less than complete if a company's network security vulnerabilities and practices are not reviewed and discussed, especially for certain types of firms. Any company involved in an acquisition

today would want to investigate the target company's network security practices as an ordinary due diligence item.

What This Means for the Public Policy Landscape: New Activity for Policy Makers

The Administration recently announced its intention to change the approach of government on managing security and critical infrastructure policymaking functions. A fresh approach that accounts for the increasing significance of the issues is most welcome. Securify is involved in many government and industry groups. From the G8 to the OECD to the Council of Europe to the US Congress to the European Commission to the Japanese Government, there is, government driven activity. From the Global Business Dialogue on Electronic Commerce (GBDe), to various industry trade associations to the newly created information sharing and analysis centers (ISACs) for key industry sectors (e.g., IT, transport, energy, finance), there is increasing senior executive level attention to these issues.

Industry remains sensitive to control of technical standards and open, global markets. Governments remain interested in setting some parameters for best practices and liability for criminal activity. Some in industry fear sharing information in industry groups as an exposure to one's competitors and to attackers. Some in industry fear sharing information with government will lead to an unauthorized disclosure and possible public embarrassment and perhaps litigation. Multinational companies and some governments

wonder how information sharing and analysis can cross borders when trust between parties may not be sufficient to address national security and espionage concerns. Many government officials and Members of Congress are concerned about foreign ownership of sensitive technologies developed here in the United States (e.g., Verio-NTT, VoiceStream-Duetsche Telekom, Silicon Valley Group-ASM Lithography (ASML), Lucent-Alcatel).

Law enforcement of course needs to have lawful access to data. Cooperation between governments and companies across borders is critical. As information sharing and analysis cooperation between government agencies and industry groups grows in the US, we will need to focus on the issue of sharing across borders. This is not a radical idea. Indeed, we can learn from our past.

Some sixty-five years ago academics, mathematicians, government intelligence specialists, cryptographers, chess masters, and others from several countries quietly gathered in Bletchley Park, England, to devise new techniques to crack the Nazi security code known as Enigma. Many governments at the time did not want to share their information or analysis with others. The British military specifically did not want to share its code breaking techniques or knowledge of the Nazi Enigma machines with the US. Churchill's political leadership broke through this barrier and harnessed the resources of the US to accelerate and expand the limited staff and materials available to Bletchley Park in war-starved England. Political leadership and coordination across

political borders is needed today to protect critical infrastructure and to build consumer and business confidence in ecommerce.

Conclusion.

The National Infrastructure Protection Center is part of the solution. Most importantly, governments will have to increase their financial and political support for improved security measures. They should start with their own networks and then the networks they connect to. Clearly, in order to strengthen our critical infrastructures from within, those networks will require greater management focus on verification and security. Otherwise they will remain weak and will continue to weaken all the networks they connect to. Greater coordination within the government and with industry will be required. Interconnectedness and network security management are challenging. But with the right technology and public policies, we can qualitatively and quantitatively diminish the threats to our critical infrastructures.

Witness Biographical Information

Dr. Taher Elgamal founded Securify, Inc. after serving as Chief Scientist at Netscape Communications where he pioneered SSL, the standard for web security. Prior to Netscape, Dr. Elgamal was the Director of Engineering at RSA Data Security, Inc. While there, he built and ran the engineering department that developed the RSA cryptographic toolkits, the industry standards for security-enabled applications and systems development. He received his Masters and PhD degrees in Computer Science from Stanford University.

A recognized leader and frequent spokesman in the information security industry, Dr. Elgamal has made numerous, substantial contributions to the industry. These include development of the original public key cryptography and digital signature technology. He invented the Elgamal cryptography technology later adopted by NIST as the digital signature standard (DSS). He also participated in the 'SET' credit card payment protocol, plus a number of Internet payment schemes.

In addition to his responsibilities as President and CEO of Securify, Dr. Elgamal serves on the board of directors of RSA Data Security, Hi/fn, Phoenix Technologies and Valicert. He resides in Silicon Valley with his wife and children. He is originally from Egypt but is a naturalized US citizen and a beneficiary of the H1-B Visa program.